Amendments to the Claims

This listing of claims will replace all prior versions, and listing, of claims in the application.

List of Claims:

Claim 1 (Canceled)

Claim 2 (Currently Amended): The method of claim [[1]] 12, further comprising creating a key window when an application is started, said key window adapted to receive a message when a file is opened and closed.

Claim 3 (Original): The method of claim 2, further comprising:
sending a message to the key window when a file is opened;
creating a child notify window associated with said file; and
creating a notify window as a child window of a document window associated with said file.

Claim 4 (Currently Amended): The method of claim [[1]] 12, further comprising:
creating a notify window when a document window is created, wherein the notify window is a child window of the document window; and
receiving by the notify window a message from the operating system when the parent document window is activated by either the application program or by action of a user.

Claim 5 (Canceled)

Claim 6 (Currently Amended): The method of claim [[5]] 12, comprising a user of an application specifying one or more rules to the application, each said rule indicating an action to be taken on said associated file before destroying said document window.

Claim 7 (Original): The method of claim 6, wherein an action includes encrypting said associated file, wherein encrypting comprises:

creating a new file containing a template of the same format as said associated file, said new file including a header, wherein said header is not encrypted;

copying to the new file a document summary in readable form;

copying to the new file visual indicia representing that the file is encrypted;

copying encrypted data from the associated file to the new file as a named stream, said encrypted data having a beginning and a length; and

writing a code to a substitute stream to prevent the new file from being written over by a user.

Claim 8 (Original): The method of claim 7, further comprising the step of including in the header a flag indicative of the type of encryption used on the associated file.

Claim 9 (Original): The method of claim 7, further comprising the step of including in the header a flag indicative of a handling procedure to be performed on said encrypted file.

Claim 10 (Original): The method of claim 7, further comprising the step of loading data from the encrypted file into a memory block containing other random data, said memory block having a beginning, wherein an offset from the beginning of the memory block of the data from the encrypted file changes each time the message monitoring program executable code is loaded.

Claim 11 (Original): The method of claim 7, further comprising the step of including in the header a flag indicative of the length of the encrypted data, and a flag that allows the message monitoring program to search for the beginning of the encrypted data.

Claim 12 (Currently Amended): A method for associating file activity of an application with the graphical display of the file on a screen comprising the steps of:

loading by an operating system an executable code of a message monitoring program adapted to monitoring a message sent by an operating system to a document display window;

establishing by the message monitoring program a system-wide window hook using available operating system API functions, said system-wide window hook associated with one or more functions in a library of said message monitoring program;

loading the message monitoring program library into the memory space of an application program, said application having been newly started and having an import table and a newly created window;

fixing the import table of the application with addresses of functions from the message monitoring program library; and

substituting the application's main window function with a message monitoring program window function;

Wherein said method further comprising, upon receipt of a document window destroy message by a document's notify window, checking for the existence of a child notify window associated with a file that was opened in association with said document, and acting upon said associated file before destroying said document window,

~~The method of claim 5,~~ wherein an action includes deleting a temporary file from a mass storage device, wherein the deletion includes the steps of wiping the device sectors of the data contained therein, and renaming the temporary file to a name consisting of one letter prior to deletion.

Claim 13 (Currently Amended): A method for associating file activity of an application with the graphical display of the file on a screen comprising the steps of:

loading by an operating system an executable code of a message monitoring program adapted to monitoring a message sent by an operating system to a document display window;

establishing by the message monitoring program a system-wide window hook using available operating system API functions, said system-wide window hook associated with one or more functions in a library of said message monitoring program;

loading the message monitoring program library into the memory space of an application program, said application having been newly started and having an import table and a newly created window;

fixing the import table of the application with addresses of functions from the message monitoring program library; and

substituting the application's main window function with a message monitoring program window function;

Wherein said method further comprising, upon receipt of a document window destroy message by a document's notify window, checking for the existence of a child notify window associated with a file that was opened in association with said document, and acting upon said associated file before destroying said document window,

wherein an action includes deleting a temporary file from a mass storage device, wherein the deletion includes the steps of wiping the device sectors of the data contained therein, and renaming the temporary file to a name consisting of one letter prior to deletion,

~~The method of claim 12,~~ wherein the wiping is performed in conformance with the standards set for in the United States National Industrial Security Program Operating Manual.

Claim 14 (Original): The method of claim 6, wherein an action includes compressing said associated file.

Claim 15 (Original): The method of claim 6, wherein an action includes translating said associated file into another language.

Claim 16 (Original): The method of claim 6, wherein an action includes converting said associated file into another file format.

Claim 17 (Original): The method of claim 6, wherein an action includes searching for a virus in said associated file.

Claim 18 (Original): The method of claim 6, wherein an action includes altering text in said associated file.

Claim 19 (Original): The method of claim 6, wherein an action includes changing or adding an optional setting to said associated file.

Claim 20 (Original): The method of claim 6, wherein an action includes spell checking said associated file.

Claim 21 (Original): The method of claim 6, wherein an action includes creating a backup of said associated file.

Claim 22 (Original): The method of claim 6, wherein an action includes versioning said associated file under a different name or stream each time said associated file is saved.

Claim 23 (Original): The method of claim 6, wherein an action includes storing said associated file content in a remote location, and storing a reference of said associated file locally.

Claim 24 (Original): The method of claim 6, wherein an action includes grammar checking said associated file.

Claim 25 (Currently Amended): The method of claim [[1]] 12, further comprising monitoring by the message monitoring program window function the creation of a document child window.

Claims 26-33 (Canceled)

Claim 34 (New): The method of claim 13, further comprising creating a key window when an application is started, said key window adapted to receive a message when a file is opened and closed.

Claim 35 (New): The method of claim 13, further comprising:
sending a message to the key window when a file is opened;
creating a child notify window associated with said file; and
creating a notify window as a child window of a document window associated with said file.

Claim 36 (New): The method of claim 13, further comprising:

creating a notify window when a document window is created, wherein the notify window is a child window of the document window; and

receiving by the notify window a message from the operating system when the parent document window is activated by either the application program or by action of a user.

Claim 37 (New): The method of claim 13, comprising a user of an application specifying one or more rules to the application, each said rule indicating an action to be taken on said associated file before destroying said document window.

Claim 38 (New): The method of claim 37, wherein an action includes encrypting said associated file, wherein encrypting comprises:

creating a new file containing a template of the same format as said associated file, said new file including a header, wherein said header is not encrypted;

copying to the new file a document summary in readable form;

copying to the new file visual indicia representing that the file is encrypted;

copying encrypted data from the associated file to the new file as a named stream, said encrypted data having a beginning and a length; and

writing a code to a substitute stream to prevent the new file from being written over by a user.

Claim 39 (New): The method of claim 38, further comprising the step of including in the header a flag indicative of the type of encryption used on the associated file.

Claim 40 (New): The method of claim 38, further comprising the step of including in the header a flag indicative of a handling procedure to be performed on said encrypted file.

Claim 41 (New): The method of claim 38, further comprising the step of loading data from the encrypted file into a memory block containing other random data, said memory block

having a beginning, wherein an offset from the beginning of the memory block of the data from the encrypted file changes each time the message monitoring program executable code is loaded.

Claim 42 (New): The method of claim 38, further comprising the step of including in the header a flag indicative of the length of the encrypted data, and a flag that allows the message monitoring program to search for the beginning of the encrypted data.

Claim 43 (New): The method of claim 37, wherein an action includes compressing said associated file.